



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/585,452

07/07/2006

Boaz Krelbaum

27512U

2799

20529 7590 01/12/2009
THE NATH LAW GROUP
112 South West Street
Alexandria, VA 22314

EXAMINER

SETO, JEFFREY K

ART UNIT

PAPER NUMBER

2446

MAIL DATE

DELIVERY MODE

01/12/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/585,452	Applicant(s) KRELBAUM ET AL.	
	Examiner Jeffrey Seto	Art Unit 2446	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 July 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 39-56,58 and 59 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 39-56,58 and 59 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07 July 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>2-08-2007</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 39-56, 58 & 59 are pending.

Priority

2. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. The effective filing date for this application is 1-07-2004.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 2-08-2007 is not in full compliance with the provisions of 37 CFR 1.97. Accordingly, the U.S. references listed in the IDS have been considered by the examiner. However, since no copies of the foreign references were provided, none of the foreign references listed in the IDS have been considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2446

4. Claims 39-44, 46-53, 55, 56, 58 & 59 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 7,415,509 issued to Kaltenmark, et al. (Kaltenmark).

5. Regarding claim 39, Kaltenmark teaches an apparatus configured to monitor and audit activity in a network, the network utilizes an incremental protocol, the apparatus comprising: a) an analyzer operative to analyze intercepted packets conveyed by entities in the network and to generate analyzed data based on information associated with at least some of said packets (See column 14, lines 19-24; wherein monitoring is accomplished by intercepting packets), the analyzed data being indicative of sessions (See column 5, lines 29-35); b) a mirror manager responsive to said analyzed data for generating mirror data representative of mirror sessions, each mirror session corresponding to one of said sessions (See col. 20, lines 62-65; wherein management data is the mirror data); and c) an audit event analyzer being responsive to said mirror data for generating event data representative of inbound audit events and outbound audit events, said event data including characteristics relating to at least on-screen field location of data being part of the inbound audit events and outbound audit events, said audit event analyzer being adapted to analyze said event data for extracting extracted data from event data representative of an inbound audit event together with the characteristics respective of said inbound audit event, and to generate event data representative of a united audit event by combining the extracted data with one or more fields in event data representative of an outbound audit event based on said

Art Unit: 2446

characteristics (See col. 20, line 65 to col. 21, line 6; wherein the event filtering generates extracted data, and event correlation produces united audit events).

6. Regarding claim 40, Kaltenmark teaches a business event analyzer for processing at least part of said event data representative of outbound, inbound and united audit events and generating data representative of business events (See col. 21, lines 6-9; wherein the management event is a business event; and See col. 12, lines 51-61).

7. Regarding claim 41, Kaltenmark teaches an alerts manager coupled to the business event analyzer and being responsive to said data representative of business events for generating alerts (See col. 21, lines 9-15).

8. Regarding claim 42, Kaltenmark teaches the alerts manager is configured to generate at least some of the alerts based on predetermined thresholds (See col. 21, lines 6-9).

9. Regarding claim 43, Kaltenmark teaches a first long term storage device for storing at least part of said analyzed data (See col. 20, lines 37-40; wherein the repositories includes a first storage device).

10. Regarding claim 44, Kaltenmark teaches a second long term storage device for storing at least part of said mirror data representative of mirror sessions (See col. 21, lines 21-24; wherein the repositories includes a second storage device).

11. Regarding claim 46, Kaltenmark teaches an encryption agent for encrypting at least part of the mirror data representative of mirror sessions (See col. 16, lines 5-6 & 63-64).

Art Unit: 2446

12. Regarding claim 47, Kaltenmark teaches a signature agent for digitally signing at least part of the mirror data representative of mirror sessions (See col. 17, lines 4-7).

13. Regarding claim 48, Kaltenmark teaches a method of monitoring and auditing activity in a network, the network utilizes an incremental protocol, the method comprising: a) analyzing intercepted packets conveyed by entities in the network (See col. 14, lines 19-24; wherein monitoring is accomplished intercepting packets); b) generating analyzed data based on information associated with at least some of said packets (See col. 20, lines 37-40), the analyzed data being indicative of sessions (See col. 5, lines 29-35); c) responsive to said analyzed data generating in respect of one or more of said sessions mirror data representative of one or more mirror sessions, each mirror session corresponding to a session (See col. 20, lines 62-65; wherein management data is the mirror data); and d) generating event data representative of inbound audit events and outbound audit events, said event data including characteristics relating to at least on-screen field location of data being part of the inbound audit events and outbound audit events (See col. 20, lines 65-67); e) extracting extracted data from event data representative of an inbound audit event together with the characteristics respective of said inbound audit event (See col. 21, lines 1-4; wherein event filtering generates extracted data); and f) generating event data representative of a united audit event by combining the extracted data with one or more fields in event data representative of an outbound audit event based on said characteristics (See col. 21, lines 3-6; wherein event correlation generates united audit events).

Art Unit: 2446

14. Regarding claim 49, this claim recites a method for operating the apparatus of claim 40, and is rejected for the same reasons.

15. Regarding claim 50, this claim recites a method for operating the apparatus of claim 41, and is rejected for the same reasons.

16. Regarding claim 51, this claim recites a method for operating the apparatus of claim 42, and is rejected for the same reasons.

17. Regarding claim 52, this claim recites a method for operating the apparatus of claim 43, and is rejected for the same reasons.

18. Regarding claim 53, this claim recites a method for operating the apparatus of claim 44, and is rejected for the same reasons.

19. Regarding claim 55, this claim recites a method for operating the apparatus of claim 46, and is rejected for the same reasons.

20. Regarding claim 56, this claim recites a method for operating the apparatus of claim 47, and is rejected for the same reasons.

21. Regarding claim 58, this claim recites a program product for carrying out the method of claim 48, and is rejected for the same reasons.

22. Regarding claim 59, Kaltenmark teaches a terminal responsive to said event data representative of a united audit event for displaying said united audit event without requiring that preceding outbound and inbound audit events be displayed prior thereto (See col. 21, lines 11-16).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

23. Claims 45 & 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaltenmark, as applied to claims 39 & 48, in view of U.S. Patent No. 5,790,798 issued to Beckett, II, et al. (Beckett).

24. Regarding claim 45, Kaltenmark teaches the invention as described in claim 39. Kaltenmark does not teach a compression agent for compressing at least part of the mirror data representative of mirror sessions. However, Beckett teaches this limitation (See column 14, lines 15-19). Using the feature of Beckett in the system of Kaltenmark would have reduced required bandwidth during transmission and reduced the amount of required memory space during storage. Therefore, it would have been obvious to one of ordinary skill, at the time of the invention, to combine the teachings of Beckett and Kaltenmark.

25. Regarding claim 54, this claim recites a method for operating the apparatus of claim 45, and is rejected for the same reasons.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey Seto whose telephone number is (571)270-7198.

Art Unit: 2446

The examiner can normally be reached on Monday thru Thursday and alt. Fridays,
9AM-6:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Pwu can be reached on (571) 273-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JKS

1/7/2009

/Joseph E. Avellino/
Primary Examiner, Art Unit 2446